NCUA 12 CFR Part 748 Overview

Summary

The National Credit Union Administration (NCUA) 12 CFR Part 748, commonly referred to as the NCUA's Security Program, Report of Crime and Catastrophic Events, and Bank Secrecy Act Compliance regulation, establishes requirements for federally insured credit unions to protect member information, ensure cybersecurity, and comply with anti-money laundering (AML) laws. Enacted under the authority of the Federal Credit Union Act and the Bank Secrecy Act (BSA), Part 748 includes three key components: the Security Program (Appendix A), Response Programs for Unauthorized Access (Appendix B), and BSA Compliance. It aligns with broader federal standards like the Gramm-Leach-Bliley Act (GLBA) and FFIEC guidelines, focusing on safeguarding nonpublic personal information (NPI), reporting suspicious activities, and responding to data breaches. Non-compliance can lead to NCUA supervisory actions, civil money penalties (up to $1 million per violation under BSA), and reputational damage. As of October 2025, updates emphasize cybersecurity incident reporting and third-party risk management. (Clarification: This is a general upper limit; actual penalties vary and are adjusted annually.)

Key Requirements

NCUA 12 CFR Part 748 is divided into three main sections with specific obligations for credit unions:

1. **Security Program (Appendix A – Guidelines for Safeguarding Member Information)**:
    - Develop and implement a written information security program, tailored to the credit union's size, complexity, and risk profile, to protect member NPI (e.g., names, account numbers, SSNs).
    - **Key Elements**:
        - Conduct risk assessments to identify threats to member information (e.g., cyberattacks, physical breaches).
        - Implement safeguards, including:
            - Encryption (e.g., AES-256) for data at rest and in transit.
            - Multi-factor authentication (MFA) for system access.
            - Access controls based on least privilege.
            - Regular security testing (e.g., vulnerability scans, penetration testing).
        - Train employees on security policies and awareness.
        - Oversee third-party service providers (e.g., IT vendors, payment processors) with contracts ensuring GLBA-compliant security.
        - Regularly evaluate and adjust the security program based on risk assessments and incidents.
    - Aligns with GLBA's Safeguards Rule and FFIEC IT Examination Handbook.

2. **Response Programs for Unauthorized Access (Appendix B – Guidance on Response Programs)**:
    - Develop a response program for unauthorized access to member information or systems.
    - **Key Actions**:
        - Contain and control incidents to prevent further unauthorized access.
        - Notify affected members promptly if misuse of NPI is reasonably possible (per 2005 Interagency Guidance).
        - File a Suspicious Activity Report (SAR) with FinCEN if the incident involves fraud or significant risk.
        - Document incidents and responses for NCUA review.
    - **2023 Update**: Report significant cybersecurity incidents to the NCUA within 72 hours (effective September 2023, per 12 CFR 748.1(c)).
3. **Bank Secrecy Act (BSA) Compliance (12 CFR 748.2)**:
    - Establish a BSA/AML compliance program, including:
        - Written policies and procedures to detect and prevent money laundering.
        - Designation of a BSA compliance officer.
        - Employee training on BSA requirements.
        - Independent testing of the BSA program (annually or per risk).
        - Customer Identification Program (CIP) to verify member identities.
    - File SARs with FinCEN for suspicious transactions (e.g., >$5,000 with suspected illegal activity).
    - Maintain records of currency transactions (CTRs) for cash transactions over $10,000.

Compliance Process:

- Annual security program reviews and updates.
- Regular NCUA examinations (aligned with FFIEC standards) to assess compliance.
- Submission of SARs/CTRs and cybersecurity incident reports to NCUA/FinCEN.
- Documentation of risk assessments, training, and incident responses.

Who Is Affected

- **Federally Insured Credit Unions**:
    - All NCUA-insured credit unions (federal and state-chartered) handling member NPI or financial transactions.
    - Includes small community credit unions and large multi-state ones.
- **Members (Consumers)**:
    - Credit union members whose NPI (e.g., account details, SSNs) is protected under the regulation.
- **Employees and Third Parties**:
    - Credit union staff (e.g., IT, compliance, tellers) managing NPI or BSA compliance.
    - Third-party vendors (e.g., core banking system providers, cloud services) must meet security standards via contracts.

- **Regulators**:
  - NCUA enforces compliance through examinations and investigations.
  - FinCEN oversees BSA/AML compliance (SARs/CTRs).
- **Impact of Non-Compliance**:
  - Civil money penalties (up to $1M per BSA violation, adjusted annually).
  - Supervisory actions (e.g., cease-and-desist orders, corrective plans).
  - Reputational damage and loss of member trust.
  - Potential loss of federal insurance for severe violations.

Relevance to Scholarships: If your scholarship program partners with a credit union for funding or disbursements (e.g., direct deposits to student accounts), NCUA 12 CFR 748 ensures secure handling of financial data. If your platform collects NPI (e.g., student bank details), align with these security standards to meet credit union requirements.

Informational Resources

- **NCUA Official Website**: ncua.gov/regulation-supervision/regulations-opinions/regulations/12-cfr-748 (full text of Part 748, Appendices A and B).
- **NCUA Cybersecurity Resources**: ncua.gov/regulation-supervision/cybersecurity (guidance, FAQs, incident reporting forms).
- **FFIEC IT Examination Handbook**: ffiec.gov/it-examination-handbooks (supplements NCUA 748 with detailed security standards).
- **FinCEN BSA Resources**: fincen.gov/resources/statutes-regulations (SAR/CTR filing guidance, BSA e-filing system).
- **Training and Tools**:
  - NCUA Cybersecurity Training Webinars: ncua.gov/regulation-supervision/training (free for credit unions).
  - FFIEC Cybersecurity Assessment Tool (CAT): ffiec.gov/cyberassessmenttool.htm (free for assessing security maturity).
  - NAFCU Compliance Resources: nafcu.org/compliance (templates for security programs, BSA policies).
- **Industry Resources**:
  - "NCUA Cybersecurity Guide" (free PDFs from vendors like CUNA or TraceSecurity).
  - Credit Union Times: credituniontimes.com (articles on 748 compliance).
  - CUNA's Cybersecurity Compliance Guide: cuna.org (checklists, risk assessment tools).
- **Community Support**:
  - NCUA Regional Workshops: ncua.gov/events (peer networking and compliance training).
  - Credit Union National Association (CUNA) forums: cuna.org (discussion groups for BSA/748 compliance).